A Study on Security in Sensor Networks

Divya James[1] , Geethu Krishna Kartha [2]

[1] *Assistant Professor,Department of Information Technology,Rajagiri School of Engineering and Technology Kochi,India*

[2] *PG Scholar,Department of Information Technology, Rajagiri School of Engineering and Technology Kochi,India*

ABSTRACT

Network Management is one of the important functionality in network Engineering. This paper proposes a methodology for security in SNMP managed sensor networks. McAfee is the platform used for implementing the security. It is mainly based on SNMP V3 which is the enhanced version of SNMP and it includes authentication.IEEE1451.4 TEDS is also incorporated to provide plug and play of sensor networks. SNMP is compactable with many kind of devices used in networking, So it provides a wide varity of devices to communicate in a network independent of the manufacturers. The proposed security method is applicable to many of the sensor devices.

Indexterms*: IEEE standard, Management Information Base, Transducers.*

I. INTRODUCTION

Networks and processing systems are of growing importance and indeed ,have become critical in business world. The management of sensor network requires many functions like configuration of sensors , security , administration etc. Simple network management protocol is an application layer protocol used for managing the network devices[1]. SNMP is a network management protocol that has become the standard for the exchange of information in a network. Before the evolution of SNMP and other network management software , administrator would have to be physically attached to the network devices in order to access the configurations and troubleshooting data[12]. It uses one or more administrative computers called managers, have the task of managing and monitoring a group of devices called managed system . software executing in each devices called agent act as an interface between manager and managed system. The manager send messages to the agent to get or set a particular object of an element. The managed devices collect and store information and make this information available to the manager system using SNMP[1]. An agent will be having management information and translate that information in to SNMP compactable form. The SNMP architecture helps to achieve the following goals[1]:

1) making the management functions more simpler
2) management and operations are comparatively more flexible
3) managing complex networks and device compatibility with the network

The SNMP provides various functions to manage the devices connected with the network using SNMP ping. Various other functions are Get Request, GetNextRequest, GetBulkRequest, SetRequest,Trap , Response , Inform Request. The manager can get information regarding a particular device by using get commanriable to retrieve the value of a variable from the list of variables. Set Request to change the value of a variable by the manager. GetNextRequest to discover the available variables and there values. GetBulkRequest to get multiple iterations of GetNextRequest by the manager. Response is send by the agent to the manager as response of any of the request messages. Trap is used by the agent to notify about alerts or special events that are to be monitored. Inform Request is send by a manager to other manager as asynchronous notifications. To access the information each device will be having a unique identifier SNMP uses dotted decimal notation called Object Identifier (OID) [2].

1.1. OTHER PROTOCOLS

CMIP :Created in 1998 by Internet Activities Board (IAB).It is more secure and powerful than SNMP But the SNMP is having very less overhead .SNMP defines only "set" actions to alter the state of managed devices while CMIP allows the definition of any kind of actions. The main feature that makes SNMP different is that it is widely available and interoperable among a variety of network components.

II. MANAGEMENT OF NETWORKS

2.1MANAGEMENT INFORMATION BASE(MIB)

MIB is defined for SNMP. It is a virtual database that helps SNMP to manage, control and monitor the devices in the network .Each SNMP variables in MIB is termed as objects.MIB defines objects through framework called structure of management information(SMI) [5].The SMI is similar to the schema of a Database system. It defines object name, data type, operations that can be performed on it. To increase the scalability all managed objects are arranged in a tree structure. The leaf nodes of the tree are the actual managed objects each of which represents some activity, resource , or related information. The MIB should be compiled after its generation in order to make the SNMP work properly. The objects in MIB are defined using Abstract syntax notation 1[2].Here hierarchical name space containing OIDs are used. The path from the top of the tree down to the point of interest forms the OID.MIB's are updated to add new functionalities , remove unwanted information and to fix defects.

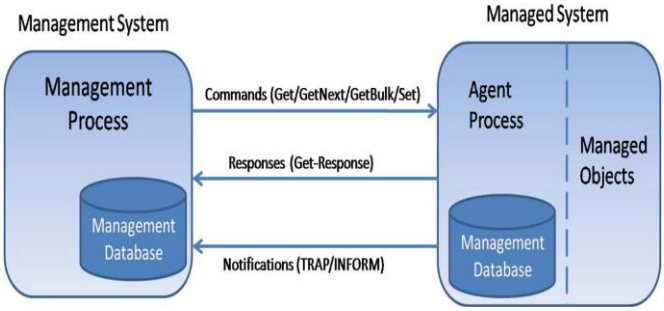

Fig1:SNMP Architecture[1]

2.2MCAFEE NETWORK SECURITY PLATFORM

Network security is one of the major aspects in computer networking. As the use of computer networks is essential part of the industries for their transactions ,the security of the system is very important[1].There are many concepts of improving or protecting network from an intruder. McAfee , the global leader in Intrusion Prevention System(IPS) provides high level security options for the system. McAfee Network Security Manager gives you real-time visibility over all McAfee intrusion prevention systems across the network. With its plug-and-play operation, easy-to-use functions Network Security Manager saves the time, trouble, and costs.

2.3IEEE 1451

The sensors must have networking capabilities that support data flow, interpretability, compatibility .security. IEEE 1451 is a new standard of managing sensor networks .It develops a vendor independent and network independent transducer interfaces. It provides many functions to make sensor smart such as[6]:

- Self-diagnostic and self-identification
- Conforming to standard data and control protocol
- Provides Standard digital data as output
- Software functions like signal processing etc

IEEE 1451.1 is Network Capable Application Model(NCAP) for smart transducer was developed in 1999 .It provides a Common Object model that can be used with multiple networking protocols. Uniform models for key functions needed in smart transducers including physical parametric data, application functionality and communication. It develops a framework that helps to create smart transducers.
IEEE1451.2 is introduced in 1997 and is known as Extensible Transducer Electronic Data Sheet (TEDS).It is basically a general calibration model for transducers. Triggering and control models define how the channel are accessed. It has a power concepts of correction engine and flexible location of correction engine and contains different kinds of sensors.IEEE 1451.3 is Digital Communication and Transducer Electronic Data Sheet (TEDS) Formats for Distributed Multidrop Systems.

IEEE1451.4 Transducer Electronic Data Sheet-used for plug and play of sensor networks.TEDS(Transducer Electronic Data Sheet) TEDS is a volatile memory inside sensor to store information. The sensor manufacturer uses this memory to store details regarding the manufacturer name, model number , serial number, sensor type and calibration data. The sensor works in two different modes such as analog and digital. In the digital mode the sensor data inside the memory can be downloaded, in the analog mode the sensor basically does the .TEDS basically is meant for plug and play of sensors. The memory in the TEDS are of two types,1)Volatile memory (RAM) 2)Permanent memory (ROM).The permanent memory stores data about the sensor manufacturer and other specification of the sensor .Volatile memory stores only the current measurement values . The IEEE 1451.4 defines TEDS as different sections chained together to form a complete TEDS. The first section is the Basic TEDS which defines the essential details regarding the sensor. Optionally , this standard template TEDS is followed by a calibration template. Two-bit selectors in the TEDS data indicate the following section. The end section of the TEDS is specified as open user area.

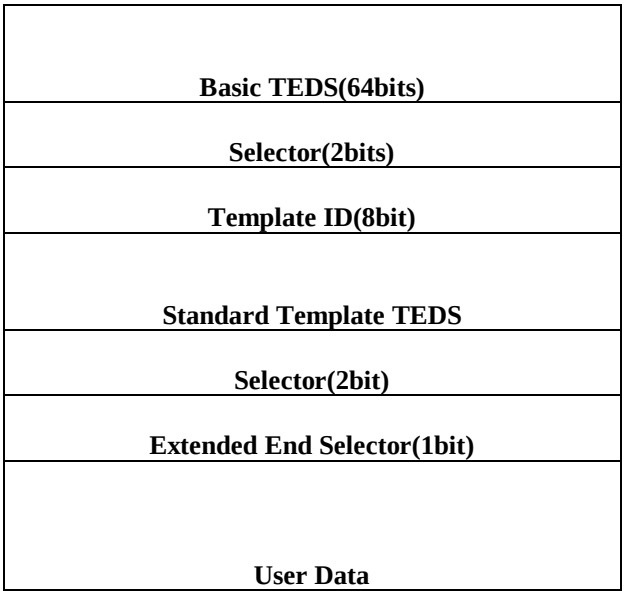

Fig2:Transducer with standard TEDS content

There are many advantages for TEDS:
1) Transducer contains data sheet information
2) No connection to PC is required
3) It can be used with many measurement points and with frequency changing configurations.
4) Makes measurements faster
5) Compactable with any kind of network and is not vendor specific.

III. RELATED WORKS

There are many papers that proposes methods for management of sensor networks. Sensor networks can be managed using Simple Network Management protocol . There are so many other protocols such as CMIP which is more effective in network management but SNMP is more simple and easy to implement. Previously there where many approaches in management of sensor networks using SNMP based MIB by considerably reducing the overhead in the network. Live Node Non-invasive Context-aware and modular Management (LiveNCM) it is a wireless sensor network management tool it is divided in to two parts one is centralized on the fixed network structure and another one, distributed on each node. Each part introduces the concept of non-invasive context aware to reduce data exchanges and diagnoses the wireless sensor node state with few messages.LiveNMC is based on Live node platform to validate energy consumptions. The main objective was to minimize the energy consumption by reducing the message exchanges. SNMP-based smart transducer interface module (STIM) is economical and scalable solution for sensor networks.

It provides a transducer independent network accessible interface, which is useable to formalize the control of devices with different functions. This MIB contains meta, meta identification, channel identification, channel, calibration, and calibration identification of TEDS information. The Entity MIB

developed in1996 uses single agent to manage multiple instances of one MIB. The Entity Sensor MIB contains a single group called the entitySensorValue group, which defines objects to convey current value and status of a physical sensor. This group contains a single table called entSensorTable, which provides a small number of READ-only objects. Management and Plug and Play of Sensor Networks Using SNMP developed in 2011 is an extension to entity sensor combines TEDS to generate a new method for management end plug and play of sensor networks. IEEE1451.4 is use to provide plug and play of sensor networks. It makes the sensor compactable with any kind of networks .The security aspects of the sensor by integrating SNMP is not implemented. IEEE 1451.4 TEDS provides the plug and play of instruments .It helps in the simplification of cable identification provides a class of templates categorizing common types of sensors. TEDS is a key feature that automates the process of inputting sensor related information . By using TEDS in defining MIB's ,it is easy to identify and manage the sensor independent of the manufacturers. This makes the sensor SNMP compatible. IEEE1451.4 will reduce the challenges associated with the sensor configurations. The entity sensor MIB can be extended to accommodate the sensor information .There are Template25 TEDS table for Template ID=25 and Template 36 TEDS table for Template ID=36 which uses Entity sensor MIB concept .

3.1.MCAFEE NETWORK SECURITY SENSORS

McAfee, the global leader in network intrusion prevention systems (IPS), delivers unprecedented levels of security offering flexible deployment options that allow organizations to optimize investment in network security. McAfee Network Security Platform provides category-best security effectiveness, scalable performance, and next-generation network IPS controls that take guesswork out of management. With Network Security Platform you get a unified network security solution for physical and virtual environments that streamlines security operations and protects your business from the latest network security threats, including malware, zero-day attacks, botnets, denial-of-service attempts, and advanced targeted attacks. It enables you to take control of your network with predictive threat intelligence, application visibility and control, network behavior analysis, and real-time threat awareness.

IV. PROPOSED MODEL

4.1 DESIGN CONSIDERATIONS

The SNMP MIB is used to store the details regarding the sensor related information. The main aim is to provide security aspects of SNMP integrated with the sensor network management. The primary goal in sensor network is to minimize the energy usage by minimizing the messages.SNMP V3 provides two types of security models User Security model and Transport Security Model. MIB is first created by using MIB editor utilities provided by the web NMS SNMP C agent. After generating the MIB design next step is to compile MIB using the tool kit. Then the Generic code can be modified based on the user requirements. Once the management system is ready next step is to provide integrated security .Here we uses McAfee network security platform for the security constraints The procedure is as shown below:

Environment

McAfee Network Security Platform

Configure the Sensor to allow an SNMP PULL and providing security:

1.Configure the SNMP v3 User:

a. Open the Network Security Manager.

b. Select the Sensor to be configured.

c. Add the account to be used by the user:

i. Select **Remote Access**, **SNMP v3 User**.

ii. Add a user with a minimum **8 character** username with authentication.

d. Add the IP address of the client that need the information of the Sensor:

i.Select the Sensor and click **Remote Access** as **Permit NMS**.

ii.Add the IP address of the client (multiple IP addresses can be added).

2. Load the Sensor MIBs.

MIBs are provided in the **NSM installation directory** in the **config** folder. The default path is **C:\Program Files\McAfee\Network Security Manager\App\config**.

The **MCAFEE-INTRUVERT-EMS-TRAP-MIB** is for the Manager, the others are for the Sensor.
a. Open your MIB Browser client.
b.Load the Sensor MIBs:
i.Select V3.
Select Algorithm MD5 and Privacy Algorithm DES.
ii.Add the username and password (previously configured in the Manager).
iii.Load the MIB.
At the top of the MIB is the entry: iso.org.dod.internet.private.enterprise.mcafee-intruvert which translates to 1.3.6.1.4.1.8962.
3.Use a command line tool to query the Sensor.
a. Open a command-line session on a Linux client.
b.Use the snmpwalk command to locate the Sensor model number. Type the command below and press ENTER:

snmpwalk –v3 –t10 –a MD5 –A <authentication-key> –x DES –X <private-key> –u <username> –l authPriv <sensor-IP> .1.3.6.1.4.1.8962.2.1.2.1.1.1
You see the Sensor model number displayed. Alternatively, you can choose the OID and pull the specific information.

4.Configure the Network Security Manager to send a trap to an SNMP manager.

a.In the Manager, select the company name from the tree on the left.
b.In the right pane, select Fault Notification, SNMP.
c.Click New.
d.Add the IP address of the SNMP manager.
e.Select the SNMP version (1 or 2). If you are unsure which version is correct, select both.
f.Select the severity level based on the alerts you want to receive.
g.Click **Finish**.
h.Open the SNMP manager and create a fault to confirm that the fault notification trap is received

This method will provide security for sensors by McAfee up to some extent.

V. CONCLUSION

The management and plug and play of sensor networks using SNMP is already implemented and Here we provide security aspects of sensor networks by integrating SNMP.Here we uses McAfee security platform which is a globally accepted IPS system. The security is provided by using SNMP V3 which have the authentication mechanism of users. But it cannot be implemented for all kinds of sensor devices.

VI. FUTUREWORK

The proposed security methodology is only applicable to some sensors. It is only supported by McAfee security systems. This can be extended to all kind of sensor devices .

REFERENCES

[1] Management and Plug and Play of Sensor Networks Using SNMP Syed Alamdar Hussain, Student Member, IEEE, and Deniz Gurkan, Member, IEEE, IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, VOL. 60, NO. 5, MAY 2011
[2] J. D.Case, M. S. Fedor, M. L. Schoffstall, and J. R. Davin, A Simple Network Management Protocol, (SNMP), DDN Network Information
Center, SRI Int., May 1990, RFC 11 57.
[3] J. Case, R. Mundy, D. Partain, and B. Stewart, Introduction to Version 3 of the Internet-Standard Network Management Framework, Apr. 1999, RFC 2570.
[4] J. Case, K. McCloghire, M. Rose, and S. Waldbusser, Introduction to Version 2 of the Internet-Standard Network Management Framework,
Apr. 1993.
[5] F. Kastenholz, SNMP Communications Services, Oct. 1991, RFC 1270.
[6] M. Rose and K. McCloghire, Structure and Identification of Management Information for TCP/IP-Based Internets, May 1990, RFC 1155.
[7] K. McCloghire and M. Rose, Management Information Base for Network
Management of TCP/IP-Based Internets: MIB-II, Mar. 1991, RFC 1213.
[8] Int. Org. Standardization, Information Processing Systems—Open Systems Interconnection—Specification of Abstract Syntax Notation One (ASN.1), Int. Std. 8824, Dec. 1987.

[9] M. Rose and K. McCloghire, Concise MIB Definitions, Mar. 1991, RFC 1212.
[10] S. Gumudavelli, D. Gurkan, and R. Wang, "Emulated network of IEEE 1451 application with multiple smart sensor reports," in Proc. IEEE
Sensor Appl. Symp., New Orleans, LA, 2009, pp. 304–308.
[11] IEEE, IEEE Standard for a Smart Transducer Interface for Sensors and Actuators—Network Capable Application Processor (NCAP) Information Model, IEEE Std. 1451.1, 1999.
[12] IEEE, IEEE Standard for A Smart Transducer Interface for Sensors and Actuators—Mixed-Mode Communication Protocols and Transducer
Electronic Data Sheet (TEDS) Formats, IEEE Std. 1451.4, 2004.
[13] A. Jacquot, J.-P. Chanet, K. M. Hou, X. Diao, and J.-J. Li, "A new approach for wireless sensor network management: LiveNCM," in Proc.
NTMS, Nov. 2008, pp. 1–6.
[14] B. Scherer, C. Toth, T. Kovacshazy, and B. Vargha, "SNMP-based approach to scalable smart transducer networks," in Proc. 20th IEEE IMTC, May 2003, pp. 721–725.
[15] K. McCloghrie and A. Bierman, Entity Management Information Base, Oct. 1996, RFC 2037.